

## **IN THE CLAIMS**

This listing of claims will replace all prior versions, and listings, of claims in the application. An identifier indicating the status of each claim is provided.

### **Listing of Claims**

1-11 (canceled)

12. (currently amended) A program distribution system for distributing a program consisting of a plurality of data elements, said program distribution system comprising:

a subscriber management system for managing subscribers' subscriptions for each program or data element;<sub>i</sub>

a subscriber authorization system for generating a scramble key to be used for descrambling said data elements contained in said program for each of said data elements;<sub>i</sub> and

a multiplexer system comprising:

an encoding system for encoding each of said data elements contained in said program to generate encoded streams consisting of encoded data elements for each program;<sub>i</sub>

a multiplexing means for multiplexing said encoded streams generated for each program by said encoding system;<sub>i</sub> and

a scramble means for selectively scrambling each of said encoded data elements contained in said multiplexed stream based on said scramble key generated by said subscriber authorization system,<sub>i</sub>

wherein said subscriber management system generates a work key for enciphering said scramble key,

wherein said subscriber authorization system comprises a first encryption means for enciphering said work key supplied as EMM data with a master key to provide an enciphered work key as an output,

wherein said multiplexer system comprises a second encryption means for enciphering said scramble key contained in ECM data with said work key to provide an enciphered scramble key as an output, and

wherein said work key used by said second encryption means for enciphering said scramble key is not said enciphered work key contained in said EMM data but an unenciphered work key obtained from a work key table supplied by said subscriber authorization system.

13- 19 (canceled)

20. (currently amended) A program distribution system according to ~~claim 19~~ claim 12, wherein said second encryption means obtains a said work key from ~~said~~ a work key identification number contained in said ECM data by referencing said work key table supplied by said subscriber authorization system, and

~~said second encryption means enciphers said scramble key contained in said ECM data by using said work key obtained from said work key table, and~~

said second encryption means provides said enciphered scramble key enciphered by said second encryption means as enciphered ECM data.

21. (currently amended) A program distribution system according to claim 20, wherein said encoded stream provided by said encoding system and ~~said~~ enciphered EMM data and ECM data

provided by said subscriber authorization system are provided in the form of transport stream packets and each of said transport stream packets is given a packet ID for identifying said transport stream packet.

22. (currently amended) A program distribution system according to claim 21, wherein said ~~multiplexer system further comprises a second encryption means for enciphering said scramble~~ key contained in said ECM data to ~~provide~~ provides enciphered ECM data as an output to said multiplexing means.

23. (currently amended) A program distribution system according to claim 22, wherein said scramble means ~~does not scramble said enciphered EMM data and said enciphered ECM data but~~ scrambles only said plurality of data elements constituting said program.

24. (original) A program distribution system according to claim 22, wherein said scramble means scrambles said data elements by using scramble keys associated with said data elements based on a table which shows the correspondence between the packet ID of a transport stream packet containing each of said data elements and a scramble key defined for said data element.

25. (original) A program distribution system according to claim 22, wherein said scramble means detects the packet IDs of all transport stream packets supplied by said multiplexing means to said scramble means,

said scramble means determines whether scramble keys are defined for said detected packet IDs based on a table which shows the correspondence between said packet IDs and said scramble keys,

if some scramble keys are defined for said packet IDs, said scramble means scrambles data elements contained in transport stream packets indicated by said packet IDs with said defined scramble keys, and

if no scramble keys are defined for said packet IDs, said scramble means does not scramble data contained in transport stream packets indicated by said packet IDs.

26. (currently amended) A program distribution system according to claim 20, wherein said multiplexer system further comprises ~~a second encryption means for enciphering said scramble key contained in said ECM data and~~ a buffer means for buffering data supplied to said multiplexer system in the form of transport stream packets and for providing said transport stream packets to said multiplexing means.

27. (original) A program distribution system according to claim 26, wherein said multiplexer system monitors free area of a plurality of buffers for buffering said transport stream packets containing said data elements, and

if any of said plurality of buffers for buffering said transport stream packets containing said data elements is likely to overflow, said transport stream packets containing said EMM data are not provided to said multiplexing means by a buffer for buffering said transport stream packets containing said EMM data and instead, said transport stream packets containing said data elements are provided to said multiplexing means by said buffer likely to overflow.

28. (currently amended) A program distribution system according to claim 20, further comprising:

a distribution system for distributing transport streams provided by said multiplexer system to the receiving end through a transmission line;<sub>1</sub> and

a reception system for receiving said transport streams transmitted through said transmission line.

29. (currently amended) A program distribution system according to claim 28, wherein said reception system comprises:

a demultiplexer for demultiplexing said transmitted transport streams;<sub>1</sub>

a descrambler for descrambling said scrambled data elements with said supplied scramble keys, respectively;<sub>1</sub>

a decoder for decoding said descrambled data for each data element;<sub>1</sub>

a CPU for analyzing transport stream packets constituting said transport stream;<sub>1</sub> and

a security module for deciphering said enciphered scramble key contained in said transport stream and supplying said deciphered scramble key to said descrambler.

30. (currently amended) A program distribution system according to claim 29, wherein said security module comprises:

a memory means for storing a subscriber's subscription information contained in said enciphered EMM data contained in said transmitted transport stream;<sub>1</sub>

a first decryption means for receiving said enciphered work key contained in said transmitted transport stream as well as the same master key as that used by said subscriber management system to decipher said enciphered work key with said master key; and

a second decryption means for receiving said enciphered scramble key contained in said transport stream as well as said deciphered work key supplied by said first decryption means to decipher said enciphered scramble key with said deciphered work key.

31. (original) A program distribution system according to claim 30, wherein said CPU filters, from said transport stream packets containing said enciphered ECM data supplied by said demultiplexer, only a transport stream packet having enciphered ECM data on a program or data element subscribed for by a subscriber, and

said CPU obtains said enciphered scramble key from said enciphered ECM data by analyzing said enciphered ECM data contained in said filtered transport stream packet.

32. (original) A program distribution system according to claim 31, wherein if an enciphered scramble key associated with said program is supplied by said CPU, said security module deciphers said supplied enciphered scramble key to supply the same scramble key to a plurality of descramblers corresponding to a plurality of data elements constituting said program, respectively, and

if a plurality of enciphered scramble keys associated with said plurality of data elements are supplied by said CPU, said security module deciphers said plurality of supplied enciphered scramble keys, respectively, to supply different scramble keys to a plurality of descramblers corresponding to subscribed data elements among said plurality of data elements.

33. (currently amended) A program distribution system for distributing a program consisting of a plurality of data elements, said program distribution system comprising:

a subscriber management system for managing subscribers' subscriptions for each program or data element;

a subscriber authorization system for generating a scramble key to be used for descrambling said data elements contained in said program for each of said data elements; and

a multiplexer system comprising:

an encoding system for encoding each of said data elements contained in said program to generate encoded streams consisting of encoded data elements for each program;

a multiplexing means for multiplexing said encoded streams generated for each program by said encoding system; and

a scramble means for selectively scrambling each of said encoded data elements contained in said multiplexed stream based on said scramble key generated by said subscriber authorization system ~~A program distribution system according to claim 12,~~

wherein said subscriber authorization system comprises a first encryption means for enciphering with a master key a work key used for enciphering said scramble key,

said subscriber authorization system supplies to said multiplexer system said enciphered work key enciphered by said first encryption means and a subscriber identification number for identifying said subscriber as enciphered EMM data, and

~~said subscriber authorization system supplies to said multiplexer system a work key identification number for identifying said enciphered work key enciphered by said encryption means and said scramble key as ECM data~~

wherein said multiplexer system further comprises, previous to said multiplexing means,  
a second encryption means for enciphering a scramble key contained in ECM data,

wherein said second encryption means obtains a work key from a work key identification  
number contained in said ECM data by referencing said work key table,

said second encryption means enciphers said scramble key contained in said ECM data  
by using said work key obtained from said work key table, and

said second encryption means supplies to said multiplexing means said enciphered  
scramble key enciphered by said second encryption means as enciphered ECM data.

34. (canceled)

35. (currently amended) A program distribution system according to claim 33, further  
comprising:

an encoder/multiplexer control system which generates a program specific information  
for identifying the packet IDs of a transport stream packet containing said plurality of data  
elements constituting said program, a transport stream packet containing said ECM data, and a  
transport stream packet containing said EMM data within a transport stream provided by said  
data distribution system, and

wherein the encoder/multiplexer control system multiplexes ~~which controls said encoder~~  
~~system and said multiplexer system to multiplex~~ said transport stream packet containing said  
plurality of data elements constituting said program, said transport stream packet containing said  
ECM data, and said transport stream packet containing said EMM data according to said  
program specific information.



36- 39 (canceled)

40. (currently amended) A program distribution system according to ~~claim 39~~ claim 35, wherein said encoder/multiplexer control system assigns to all transport stream packets supplied to said multiplexer system in the form of transport stream packets, packet IDs for identifying said transport stream packets.

41. (original) A program distribution system according to claim 40, wherein said program specific information consists of at least a program association table, a program map table, and a conditional access table.

42. (original) A program distribution system according to claim 41, wherein said encoder/multiplexer control system supplies to said multiplexer system a transport stream packet containing said program association table as a PAT packet,

said encoder/multiplexer control system supplies to said multiplexer system a transport stream packet containing said program map table as a PMT packet, and

said encoder/multiplexer control system supplies to said multiplexer system a transport stream packet containing said conditional access table as a CAT packet.

43. (currently amended) A program distribution system according to claim 42, wherein said program association table is a table for specifying a program number and the packet ID of a PMT packet corresponding to said program number,

said program map table is a table for specifying the packet ID of a transport stream packet containing each of a plurality of data elements constituting a program, and

said conditional access table is a table for specifying the packet ID of ~~said~~ an enciphered EMM packet.

44. (original) A program distribution system according to claim 43, wherein said program association table describes the program number for indicating a program and the packet ID of a PMT packet associated with said program, and

said program map table describes the program number for indicating said program, a plurality of packet IDs containing transport stream packets containing a plurality of data elements constituting said program, and a descriptor for specifying the packet ID of an enciphered ECM packet associated with said program or said data element.

45. (original) A program distribution system according to claim 44, wherein if said descriptor in said program map table is described at a location corresponding to said program number, said descriptor specifies the packet ID of an ECM packet containing a scramble key for scrambling all data elements of said plurality of data elements constituting said program, and

if said descriptor in said program map table is described at a location corresponding to each of said data elements of said program, said descriptor specifies the packet IDs of a plurality of ECM packets containing a plurality of scramble keys for scrambling said plurality of data elements constituting said program, respectively.

46. (original) A program distribution system according to claim 45, wherein if said program has a first data element through an n'th data element and the same scramble key is specified for said first data element through said n'th data element,

said program map table describes the correspondence between the program number for indicating said program and the packet IDs of ECM packets containing scramble keys for scrambling said first data element through said n'th data element, respectively.

47. (original) A program distribution system according to claim 45, wherein if said program has a first data element through an n'th data element and at least one different scramble key is specified for said first data element through said n'th data element,

said program map table describes the correspondence between the packet ID of a transport stream packet containing said first data element and the packet ID of a transport stream packet containing ECM data containing a scramble key for scrambling said first data element, and

said program map table describes the correspondence between the packet ID of a transport stream packet containing said n'th data element and the packet ID of a transport stream packet containing ECM data containing a scramble key for scrambling said n'th data element.

48. (original) A program distribution system according to claim 42, wherein said encoder/multiplexer control system specifies unique packet IDs for said program map table and said conditional access table.

49. (original) A program distribution system according to claim 42, wherein said scramble means does not scramble said program specific information, said EMM data, and said ECM data but scrambles only said data elements.

50. (original) A program distribution system according to claim 42, wherein said scramble means scrambles said data elements by using scramble keys specified for said data elements based on a table which shows the correspondence between the packet ID of a transport stream packet containing each of said data elements and a scramble key specified for said data element.

51. (original) A program distribution system according to claim 42, wherein said encoder/multiplexer control system stores packet IDs used for previous operations so that repetitive assignment at a packet ID to a plurality of transport stream packets can be avoided when packet IDs are specified to identify said ECM packet, said EMM packet, said PSI packet, and said elementary packet, respectively.

52. (original) A program distribution system according to claim 42, wherein said encoder/multiplexer control system generates a table which shows the correspondence between the packet ID assigned to each transport stream packet and a scramble key used for scrambling data contained in said transport stream packet, and

said encoder/multiplexer control system supplies to said multiplexer system said table for showing the correspondence between said packet IDs and said scramble keys.

53. (original) A program distribution system according to claim 52, wherein said scramble means does not scramble said program specific information, said EMM data, and said ECM data but scrambles only said data elements by referencing said table for showing the correspondence between said packet IDs and said scramble keys.

54. (original) A program distribution system according to claim 52, wherein said scramble means scrambles said data elements with scramble keys specified for said data elements by referencing said table for showing the correspondence between said packet IDs and said scramble keys.

55. (original) A program distribution system according to claim 52, wherein said scramble means detects the packet IDs of all transport stream packets supplied by said multiplexing means to said scramble means,

said scramble means determines whether scramble keys are defined for said detected packet IDs based on said table which shows the correspondence between said packet IDs and said scramble keys,

if some scramble keys are defined for said packet IDs, said scramble means scrambles data elements contained in transport stream packets indicated by said packet IDs with said defined scramble keys, and

if no scramble keys are defined for said packet IDs, said scramble means does not scramble data contained in transport stream packets indicated by said packet IDs.

56. (currently amended) A program distribution system according to ~~claim 36~~ claim 33, wherein said multiplexer system further comprises:

~~a second encryption means for enciphering said scramble keys, and~~

a plurality of buffer means for buffering said-PAT packets, said-PMT packets, said-CAT packets, said-transport stream packets containing said data elements, said-enciphered EMM packets, and said-enciphered ECM packets, respectively, and for providing said transport stream packets to said multiplexing means.

57. (original) A program distribution system according to claim 56, wherein said multiplexer system monitors free area of a plurality of buffers for buffering said transport stream packets containing said data elements, and

if any of said plurality of buffers for buffering said transport stream packets containing said data elements is likely to overflow, said EMM packets are not provided to said multiplexing means by a buffer for buffering said EMM packets and instead, said transport stream packets containing said data elements are provided to said multiplexing means by said buffer likely to overflow.

58. (original) A program distribution system according to claim 47, further comprising:

a distribution system for distributing transport streams provided by said multiplexer system to the receiving end through a transmission line, and

a reception system for receiving said transport streams transmitted through said transmission line.

59. (currently amended) A program distribution system according to claim 58, wherein said reception system comprises:

a demultiplexer for demultiplexing said transmitted transport streams;

a descrambler for descrambling said scrambled data elements with said supplied scramble keys, respectively;

a decoder for decoding said descrambled data for each data element;

a CPU for analyzing transport stream packets constituting said transport stream; and

a security module for deciphering said enciphered scramble key contained in said transport stream and supplying said deciphered scramble key to said descrambler.

60. (currently amended) A program distribution system according to claim 59, wherein said CPU comprises:

a PAT analyzing means for analyzing a program association table contained in said transport stream;

a PMT analyzing means for analyzing a program map table contained in said transport stream;

a CAT analyzing means for analyzing a conditional access table contained in said transport stream;

an EMM analyzing means for analyzing enciphered EMM data contained in said transport stream; and

an ECM analyzing means for analyzing enciphered ECM data contained in said transport stream.

61. (currently amended) A program distribution system according to claim 59, wherein said security module comprises:

a memory means for storing a subscriber's subscription information contained in said EMM data;

a first decryption means for receiving said enciphered work key contained in said transmitted transport stream as well as the same master key as that used by said subscriber management system to decipher said enciphered work key with said master key; and

a second decryption means for receiving said enciphered scramble key contained in said transport stream as well as said deciphered work key supplied by said first decryption means to decipher said enciphered scramble key with said deciphered work key.

62. (original) A program distribution system according to claim 61, wherein said CPU identifies a transport stream packet containing each of data elements constituting said program by analyzing a program association table and a program map table contained in said transport stream and controls said demultiplexer to provide said transport stream packet containing said data element to appropriate one of said scramblers.

63. (original) A program distribution system according to claim 62, wherein said CPU detects a transport stream packet containing EMM data by analyzing a conditional access table contained in said transport stream,

said CPU filters, from said transport stream containing said EMM data, only a transport stream packet having EMM data on a program subscribed for by a subscriber, and

said CPU obtains said enciphered work key from said EMM data by analyzing said EMM data contained in said filtered transport stream packet.



64. (original) A program distribution system according to claim 61, wherein said CPU detects transport stream packets containing a plurality of data elements constituting said program and said ECM data, respectively, by analyzing a program association table contained in said transport stream and a program map table specified by said program association table, and

said CPU controls said demultiplexer to supply said transport stream packets containing said plurality of data elements to said descramblers, respectively, and to receive said transport stream packet containing said ECM data.

65. (original) A program distribution system according to claim 64, wherein said CPU filters, from said transport stream packets containing said enciphered ECM data supplied by said demultiplexer, only a transport stream packet having enciphered ECM data on a program or data element subscribed for by a subscriber, and

said CPU obtains said enciphered scramble key from said enciphered ECM data by analyzing said enciphered ECM data contained in said filtered transport stream packet.

66. (original) A program distribution system according to claim 65, wherein if the correspondence between said program number and the packet ID of said enciphered ECM packet is described according to the syntax of said program map table,

said CPU supplies to said security module an enciphered scramble key contained in said enciphered ECM packet specified by said packet ID as an enciphered scramble key corresponding to said program, and

if the correspondence between a plurality of data elements constituting said program and the packet IDs of said plurality of enciphered ECM packets is described according to the syntax of said program map table,

said CPU supplies to said security module a plurality of different scramble keys contained in said enciphered ECM packets specified by said plurality of packet IDs as enciphered scramble keys corresponding to said plurality of data elements.

67. (original) A program distribution system according to claim 66, wherein if an enciphered scramble key associated with said program is supplied by said CPU, said security module deciphers said supplied enciphered scramble key to supply the same scramble key to a plurality of descramblers corresponding to a plurality of data elements constituting said program, respectively, and

if a plurality of enciphered scramble keys associated with said plurality of data elements are supplied by said CPU, said security module deciphers said plurality of supplied enciphered scramble keys, respectively, to supply different scramble keys to a plurality of descramblers corresponding to subscribed data elements among said plurality of data elements.

68-70 (canceled)

71. (currently amended) A program transmission method for transmitting a program consisting of a plurality of data elements, said method comprising:

a scramble key generation step for generating a plurality of scramble keys to be used for scrambling a plurality of data elements contained in said program so that a subscriber can watch and/or hear only programs or data elements subscribed for by said subscriber;

an encoding step for encoding each of said data elements contained in said program to generate encoded streams consisting of encoded data elements for each program;

a multiplexing step for multiplexing said encoded streams provided for each program by said encoding step; and

a scramble step for selectively scrambling each of said encoded data elements contained in said multiplexed stream based on said generated scramble key,

wherein said multiplexing step comprises an encryption step for enciphering a scramble key contained in ECM data,

wherein said scramble key generation step generates a work key table which shows the correspondence between said work key and a work key identification number for identifying said work key,

wherein said encryption step in said multiplexing step obtains a work key from said work key identification number contained in said ECM data by referencing said work key table,

said encryption step enciphers said scramble key contained in said ECM data by using said work key obtained from said work key table, and

said encryption step provides said enciphered scramble key enciphered by said second encryption circuit as enciphered ECM data.

72-77 (canceled)

78. (currently amended) A program transmission method according to ~~claim 77~~ claim 71, further comprising a wherein said program specific information generation step for assigning assigns to all transport stream packets ~~supplied to said multiplexer system in the form of transport stream packets,~~ packet IDs for identifying said transport stream packets.

79. (original) A program transmission method according to claim 78, wherein said program specific information consists of at least a program association table, a program map table, and a conditional access table.

80. (currently amended) A program transmission method according to claim 79, wherein said program specific information generation step supplies to said ~~multiplexer system~~ multiplexing step a transport stream packet containing said program association table as a PAT packet,

said program specific information generation step supplies to said ~~multiplexer system~~ to said multiplexing step a transport stream packet containing said program map table as a PMT packet, and

said program specific information generation step supplies to said ~~multiplexer system~~ to said multiplexing step a transport stream packet containing said conditional access table as a CAT packet.

81. (original) A program transmission method according to claim 80, wherein said program association table is a table for specifying a program number and the packet ID of a PMT packet corresponding to said program number,

said program map table is a table for specifying the packet ID of a transport stream packet containing each of a plurality of data elements constituting a program, and

said conditional access table is a table for specifying the packet ID of said enciphered EMM packet.

82. (original) A program transmission method according to claim 81, wherein said program association table describes the program number for indicating a program and the packet ID of a PMT packet associated with said program, and

said program map table describes the program number for indicating said program, a plurality of packet IDs containing transport stream packets containing a plurality of data elements constituting said program, and a descriptor for specifying the packet ID of an enciphered ECM packet associated with said program or said data element.

83. (original) A program transmission method according to claim 82, wherein if said descriptor in said program map table is described at a location corresponding to said program number, said descriptor specifies the packet ID of an ECM packet containing a scramble key for scrambling all data elements of said plurality of data elements constituting said program, and

if said descriptor in said program map table is described at a location corresponding to each of said data elements of said program, said descriptor specifies the packet IDs of a plurality of ECM packets containing a plurality of scramble keys for scrambling said plurality of data elements constituting said program, respectively.

84. (original) A program transmission method according to claim 83, wherein if said program has a first data element through an n'th data element and at least one different scramble key is specified for said first data element through said n'th data element,

said program map table describes the correspondence between the packet ID of a transport stream packet containing said first data element and the packet ID of a transport stream

packet containing ECM data containing a scramble key for scrambling said first data element,  
and

said program map table describes the correspondence between the packet ID of a transport stream packet containing said n'th data element and the packet ID of a transport stream packet containing ECM data containing a scramble key for scrambling said n'th data element.

85. (currently amended) A program transmission method according to claim 80, wherein said scramble step does not scramble said program specific information, said EMM data, and said ECM data but scrambles only said data elements by using scramble keys specified for said data elements based on a table which shows the correspondence between the packet ID of a transport stream packet containing each of said data elements and a scramble key specified for said data element.

86. (currently amended) A program transmission method according to claim 80, wherein said program specific information generation step generates a table which shows the correspondence between the packet ID assigned to each transport stream packet and a scramble key used for scrambling data contained in said transport stream packet, and

said program specific information generation step supplies to said multiplexing step ~~to said multiplexer system~~ said table for showing the correspondence between said packet IDs and said scramble keys.

87. (currently amended) A program transmission method according to claim 86, wherein said scramble means does not scramble said program specific information, ~~said~~ EMM data, and said

ECM data but scrambles only said data elements by referencing said table for showing the correspondence between said packet IDs and said scramble keys.

88. (original) A program transmission method according to claim 86, wherein said scramble step detects the packet IDs of all transport stream packets supplied by said multiplexing means to said scramble means,

said scramble step determines whether scramble keys are defined for said detected packet IDs based on said table which shows the correspondence between said packet IDs and said scramble keys,

if some scramble keys are defined for said packet IDs, said scramble step scrambles data elements contained in transport stream packets indicated by said packet IDs with said defined scramble keys, and

if no scramble keys are defined for said packet IDs, said scramble step does not scramble data contained in transport stream packets indicated by said packet IDs.

89. (currently amended) A program transmission method according to ~~claim 74~~ claim 71, wherein said multiplexing step enciphers said scramble keys with said work key, and

said multiplexing step buffers ~~said~~-PAT packets, ~~said~~-PMT packets, ~~said~~-CAT packets, ~~said~~-transport stream packets containing said data elements, ~~said~~-enciphered EMM packets, and ~~said~~-enciphered-ECM packets in a plurality of buffer means, respectively.

90. (currently amended) A program transmission method according to claim 89, wherein said multiplexing step monitors free area of a plurality of buffers for buffering said transport stream packets containing said data elements, and

if any of said plurality of buffers for buffering said transport stream packets containing said data elements is likely to overflow, said EMM packets are not provided to said multiplexing ~~step means~~ by a buffer for buffering said EMM packets and instead, said transport stream packets containing said data elements are provided by said buffer likely to overflow.

91. (currently amended) A conditional access system for providing a conditional access to only subscribed programs and data elements among a plurality of programs and a plurality of data elements constituting said programs distributed by a program distribution system, ~~said conditional access system comprising:~~

wherein said program distribution system comprises:

a subscriber authorization system for generating a plurality of scramble keys to be used for scrambling data elements contained in said program so that a subscriber can watch and/or hear only data programs or elements subscribed for by said subscriber,

wherein said subscriber authorization system comprises a first encryption means for enciphering a work key used for enciphering said scramble key with a master key;

said conditional access system comprising:

a demultiplexer means for demultiplexing, from a said transport stream, a transport stream packet containing a plurality of the scrambled data elements constituting said program and for demultiplexing a plurality of transport stream packets containing a plurality of enciphered scramble keys associated with said plurality of data elements;



a filter means for filtering, from said plurality of transport stream packets containing said plurality of demultiplexed enciphered scramble keys, a transport stream packet containing an enciphered scramble key associated with said programs and data elements subscribed for by a subscriber;

a decryption means for deciphering said plurality of enciphered scramble keys contained in said plurality of filtered transport stream packets to generate a plurality of deciphered scramble keys;

a descramble means for descrambling said plurality of demultiplexed data elements for each data element by using said plurality of deciphered scramble keys associated with said plurality of data elements; and

a decoding means for decoding said plurality of data elements descrambled by said descramble means; and

a multiplexer system having a second encryption means for enciphering a scramble key contained in ECM data,

wherein said subscriber authorization system supplies to said second encryption means of said multiplexer system a work key table which shows the correspondence between said work key and a work key identification number for identifying said work key,

wherein said second encryption means obtains a work key from said work key identification number contained in said ECM data by referencing said work key table,

said second encryption means enciphers said scramble key contained in said ECM data by using said work key obtained from said work key table, and

said second encryption means supplies to said multiplexing system said enciphered scramble key enciphered by said second encryption means as enciphered ECM data.

92- 98 (canceled)

99. (currently amended) A conditional access system according to ~~claim 98~~ claim 91, further comprising an ~~wherein said~~ encoder/multiplexer control system that assigns to all transport stream packets supplied to said multiplexer system in the form of transport stream packets, packet IDs for identifying said transport stream packets.

100. (currently amended) A conditional access system according to claim 99, further comprising ~~wherein said~~ program specific information that consists of at least a program association table, a program map table, and a conditional access table.

101. (original) A conditional access system according to claim 100, wherein said encoder/multiplexer control system supplies to said multiplexer system a transport stream packet containing said program association table as a PAT packet,

said encoder/multiplexer control system supplies to said multiplexer system a transport stream packet containing said program map table as a PMT packet, and

said encoder/multiplexer control system supplies to said multiplexer system a transport stream packet containing said conditional access table as a CAT packet.

102. (currently amended) A conditional access system according to claim 101, wherein said program association table is a table for specifying a program number and the packet ID of a PMT packet corresponding to said program number,

said program map table is a table for specifying the packet ID of a transport stream packet containing each of a plurality of data elements constituting a program, and

said conditional access table is a table for specifying the packet ID of ~~said an~~ enciphered EMM packet.

103. (original) A conditional access system according to claim 102, wherein said program association table describes the program number for indicating a program and the packet ID of a PMT packet associated with said program, and

said program map table describes the program number for indicating said program, a plurality of packet IDs containing transport stream packets containing a plurality of data elements constituting said program, and a descriptor for specifying the packet ID of an enciphered ECM packet associated with said program or said data element.

104. (original) A conditional access system according to claim 103, wherein if said descriptor in said program map table is described at a location corresponding to said program number, said descriptor specifies the packet ID of an ECM packet containing a scramble key for scrambling all data elements of said plurality of data elements constituting said program, and

if said descriptor in said program map table is described at a location corresponding to each of said data elements of said program, said descriptor specifies the packet IDs of a plurality of ECM packets containing a plurality of scramble keys for scrambling said plurality of data elements constituting said program, respectively.

105. (original) A conditional access system according to claim 104, wherein if said program has a first data element through an n'th data element and at least one different scramble key is specified for said first data element through said n'th data element,

said program map table describes the correspondence between the packet ID of a transport stream packet containing said first data element and the packet ID of a transport stream packet containing ECM data containing a scramble key for scrambling said first data element, and

said program map table describes the correspondence between the packet ID of a transport stream packet containing said n'th data element and the packet ID of a transport stream packet containing ECM data containing a scramble key for scrambling said n'th data element.

106. (currently amended) A conditional access system according to claim 101, wherein said scramble means does not scramble said program specific information, ~~said~~ EMM data, and said ECM data but scrambles only said data elements by using scramble keys specified for said data elements based on a table which shows the correspondence between the packet ID of a transport stream packet containing each of said data elements and a scramble key specified for said data element.

107. (original) A conditional access system according to claim 101, wherein said encoder/multiplexer control system generates a table which shows the correspondence between the packet ID assigned to each transport stream packet and a scramble key used for scrambling data contained in said transport stream packet, and

said encoder/multiplexer control system supplies to said multiplexer system said table for showing the correspondence between said packet IDs and said scramble keys.

108. (currently amended) A conditional access system according to claim 107, wherein said scramble means does not scramble said program specific information, ~~said~~ EMM data, and said ECM data but scrambles only said data elements by referencing said table for showing the correspondence between said packet IDs and said scramble keys.

109. (currently amended) A conditional access system according to claim 107, wherein said scramble means detects the packet IDs of all transport stream packets supplied by said ~~multiplexing means~~ to said scramble means,

said scramble means determines whether scramble keys are defined for said detected packet IDs based on said table which shows the correspondence between said packet IDs and said scramble keys,

if some scramble keys are defined for said packet IDs, said scramble means scrambles data elements contained in transport stream packets indicated by said packet IDs with said defined scramble keys, and

if no scramble keys are defined for said packet IDs, said scramble means does not scramble data contained in transport stream packets indicated by said packet IDs.

110. (currently amended) A conditional access system according to ~~claim 95~~ claim 91, wherein said multiplexer system further comprises:

~~a second encryption means for enciphering said scramble keys, and~~

a plurality of buffer means for buffering ~~said~~-PAT packets, ~~said~~-PMT packets, ~~said~~-CAT packets, ~~said~~-transport stream packets containing said data elements, ~~said~~-enciphered EMM packets, and ~~said~~-enciphered ECM packets, respectively, and for providing said transport stream packets to said multiplexing ~~means~~ system.

111. (currently amended) A conditional access system according to claim 110, wherein said multiplexer system monitors free area of a plurality of buffers for buffering said transport stream packets containing said data elements, and

if any of said plurality of buffers for buffering said transport stream packets containing said data elements is likely to overflow, said EMM packets are not provided to said multiplexing ~~means~~ system by a buffer for buffering said EMM packets and instead, said transport stream packets containing said data elements are provided to said multiplexing ~~means~~ system by said buffer likely to overflow.

112. (currently amended) A conditional access system according to claim 109, wherein said filter means comprises:

a PAT analyzing means for analyzing a program association table contained in said transport stream;

a PMT analyzing means for analyzing a program map table contained in said transport stream;

a CAT analyzing means for analyzing a conditional access table contained in said transport stream;

an EMM analyzing means for analyzing enciphered EMM data contained in said transport stream; and

an ECM analyzing means for analyzing enciphered ECM data contained in said transport stream.

113. (currently amended) A conditional access system according to claim 109, wherein said decryption means comprises:

a memory means for storing a subscriber's subscription information contained in said EMM data;

a first decryption means for receiving said enciphered work key contained in said transmitted transport stream as well as the same master key as that used by said subscriber management system to decipher said enciphered work key with said master key; and

a second decryption means for receiving said enciphered scramble key contained in said transport stream as well as said deciphered work key supplied by said first decryption means to decipher said enciphered scramble key with said deciphered work key.

114. (original) A conditional access system according to claim 113, wherein said demultiplexer means and said filter means identify a transport stream packet containing each of data elements constituting said program by analyzing a program association table and a program map table contained in said transport stream and control said demultiplexer to provide said transport stream packet containing said data element to appropriate one of said scramblers.

115. (original) A conditional access system according to claim 114, wherein said demultiplexer means and said filter means detect a transport stream packet containing EMM data by analyzing a conditional access table contained in said transport stream,

said demultiplexer means and said filter means filter, from said transport stream containing said EMM data, only a transport stream packet having EMM data on a program subscribed for by a subscriber, and

said demultiplexer means and said filter means obtain said enciphered work key from said EMM data by analyzing said EMM data contained in said filtered transport stream packet.

116. (original) A conditional access system according to claim 113, wherein said demultiplexer means and said filter means detect transport stream packets containing a plurality of data elements constituting said program and said ECM data, respectively, by analyzing a program association table contained in said transport stream and a program map table specified by said program association table, and

said demultiplexer means and said filter means control said demultiplexer to supply said transport stream packets containing said plurality of data elements to said descramblers, respectively, and to receive said transport stream packet containing said ECM data.

117. (original) A conditional access system according to claim 116, wherein said demultiplexer means and said filter means filter, from said transport stream packets containing said enciphered ECM data supplied by said demultiplexer, only a transport stream packet having enciphered ECM data on a program or data element subscribed for by a subscriber, and



said demultiplexer means and said filter means obtain said enciphered scramble key from said enciphered ECM data by analyzing said enciphered ECM data contained in said filtered transport stream packet.

118. (original) A conditional access system according to claim 117, wherein if the correspondence between said program number and the packet ID of said enciphered ECM packet is described according to the syntax of said program map table,

said filter means supplies to said decryption means an enciphered scramble key contained in said enciphered ECM packet specified by said packet ID as an enciphered scramble key corresponding to said program, and

if the correspondence between a plurality of data elements constituting said program and the packet IDs of said plurality of enciphered ECM packets is described according to the syntax of said program map table,

said filter means supplies to said decryption means a plurality of different scramble keys contained in said enciphered ECM packets specified by said plurality of packet IDs as enciphered scramble keys corresponding to said plurality of data elements.

119. (original) A conditional access system according to claim 118, wherein if an enciphered scramble key associated with said program is supplied by said filter means, said decryption means deciphers said supplied enciphered scramble key to supply the same scramble key to a plurality of descramblers corresponding to a plurality of data elements constituting said program, respectively, and

if a plurality of enciphered scramble keys associated with said plurality of data elements are supplied by said filter means, said decryption means deciphers said plurality of supplied enciphered scramble keys, respectively, to supply different scramble keys to a plurality of descramblers corresponding to subscribed data elements among said plurality of data elements.

120-122 (canceled)